Висновок. Наведені в доповіді результати дослідження полягають в тому, що авторами вперше сформульовані принципи побудови мережі комп'ютерної контролю та супроводженню вантажоперевезень на залізниці, що, за рахунок більш чіткого визначення місця скоєння злочину, підвищить ефективність розкриття злочину. Розроблена нова класифікація типових слідчих ситуацій, в залежності від місця отримання інформацій про нестачу вантажу (ВКП), дозволяє вірно визначати набір невідкладних слідчих дій при розслідуванні крадіжки вантажів на залізниці.

Література

1. Results of work of the bodies and units of the Ministry of Internal Affairs of Ukraine for the control of theft of goods and disassembly of rolling stock at the Pridniprovs'ka railway. [Text]. Dnipro: BWRW of the Ministry of Internal Affairs of Ukraine. (in Ukrainian).
2. Kroon L., Maroti, G., & Nielsen, L., (2014). Rescheduling of railway rolling stock with dynamic passenger flows. *Transportation Science,* 49(2), 165-184pp
3. Lomako M., Timoshenko P.Yu. Application of technical instrumentality in the activity of operational officers of internal affairs for the prevention and documentation of offenses. K.: 2004, p.17-26.
4. Forensic methodology for investigating certain types of crimes. Edited by A.P Rezvan M.: IMC GUK of the Ministry of Internal Affairs of Russia. 2002 p.225-226.
5. Vishnya V.B., Specialize in the development of the cradle of wardens in the hall of transport [Text], V.B. Vishnya., *Scientific Herald of Dnipropetrovsk State University of Internal Information:* Collection of Sciences works-2015. №2. 315-322pp
6. The way of the control of the burial-ground vantage-carrying on the hall. [Text]: *Declaration. patent* № 8927. Ukraine. IPC 7 B61L13 / 00 / O.V.Vishnya. - No. 200503376; Declared on April 11, 2005; 15.08.2005, Bul. № 8. (in Ukrainian).
7. Vishnya V.B., Typical investigative situations for the investigation of robbery abductions in the use of the network of control of freight transportation on the railways [Text], V.B.Vishnya, O.V. Zelenina, *Scientific Bulletin of the Dnipropetrovsk State University of Internal Affairs*: Coll. sciencсs works. 2017. No. 1 WITH. 221-226pp. (in Ukrainian).

Способи та методи попередження та протидії легалізації доходів, одержаних у сфері кіберзлочинності

Ковтун В.О.
курсант 2 курсу групи Ф4-202 факультету № 4 (кіберполіції)
Харківського національного університету внутрішніх справ
Світличний В.А.
доцент кафедри інформаційних технологій та кібербезпеки
Харківського національного університету внутрішніх справ
к.т.н., доцент

Поняття «кіберзлочинність» вперше з'явилось в американській, а потім і в іншій іноземній літературі на початку 1960-х рр. і визначалося як порушення чужих прав та інтересів по відношенню до автоматизованих систем обробки даних [1].

Згідно з Законом України «Про основні засади забезпечення кібербезпеки України» кіберзлочинність - сукупність кіберзлочинів. Кіберзлочин (комп'ютерний злочин) – суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України [2].

Найбільш поширеними способами відмивання злочинних доходів, які використовують в своїй діяльності кіберзлочинці, є:

- перерахування коштів на карткові та корпоративні рахунки фізичних осіб з подальшим зняттям готівкою, в тому числі через банкомати тощо;
- переміщення коштів через рахунки фізичних та юридичних осіб, з подальшим придбанням товарів та послуг через Інтернет;
- переведення коштів в електронні гроші та подальше обготівковування або придбання товарів;
- обмін/розміщення коштів на електронних гаманцях [3].

Попередження кіберзлочинності базується на заходах спрямованих на зниження ризику здійснення таких злочинів та нейтралізацію шкідливих наслідків для суспільства та приватного сектору. Ефективна протидія кіберзлочинам повинна поєднувати комплекс правових (законодавчих), технічних, організаційних та інформаційних заходів [4].

Вдосконалення нормативно-правового забезпечення у сфері попередження та протидії легалізації доходів, пов'язаних із злочинами у сфері кіберзлочинності, можливе за наступними напрямами:

- внесення змін до КК України в частині посилення відповідальності за злочини у сфері комп'ютерних та інформаційних технологій;
- визнання електронних документів та інших даних у якості доказової бази при розслідуванні кіберзлочинів;
- введення сертифікації електронних платіжних засобів;
- обов'язку банків встановити антискімингові пристрої на всіх банкоматах тощо.

З метою попередження кіберзлочинів банківськими установами можуть впроваджуватись наступні технічні та організаційні заходи:

- періодичний огляд банкоматів для виявлення незаконно встановлених пристроїв;
- вимоги щодо двофакторної/двоканальної аутентифікації;
- обов'язкове інформування клієнтів про кожну проведену операцію;
- підтвердження платежу в телефонному режимі тощо.

У зв'язку з цим, значну користь у попередженні кіберзлочинності, мають інформаційно-просвітницькі заходи щодо нових ризиків та загроз в інформаційних та комп'ютерних системах [5].

Висновки: протидія кіберзлочинам поєднує комплекс правових, технічних, організаційних та інформаційних заходів, при цьому роль кожного з цих заходів не може бути визначена пріоритетною чи другорядною. При цьому ефективна протидія відмиванню злочинних доходів та зниження рівня злочинності в цій сфері можливі завдяки своєчасному виявленню фінансових операцій, що можуть бути пов'язані з відмивання доходів, одержаних у сфері кіберзлочинності, та ефективному співробітництву між державним та приватним сектором.

Література:

1. Н. Міщук Кіберзлочинність як загроза інформаційному суспільству. *Вісник Львівського університету - Серія економічна* URL: http://publications.lnu.edu.ua/bulletins/index.php/economics/article/view/5886/5899
2. «Про основні засади забезпечення кібербезпеки України» : Закон України від 05.10.2017 // БД «Законодавство України / ВР України. URL: https://zakon.rada.gov.ua/laws/show/2163-19/ed20171005#n15
3. Схеми: Легалізація коштів від кіберзлочинів // Академія фінансового моніторингу 05.04.2019 URL: https://finmonitoring.in.ua/sxemi-legalizaciya-koshtiv-vid-kiberzlochiniv/
4. Про затвердження Типологій легалізації (відмивання) доходів, одержаних злочинним шляхом, у 2013 році : Наказ від 25.12.2013 № 157. БД «Законодавство України / ВР України. URL: https://zakon.rada.gov.ua/rada/show/v0157827-13
5. Департамент фінансових розслідувань Державна служба фінансового моніторингу України Кіберзлочинність та відмивання коштів URL: http://www.sdfm.gov.ua/content/file/Site_docs/2013/20131230/tipolog2013.pdf

Рекомендації щодо основних шляхів створення належного рівня захищеності Єдиної інформаційної системи МВС України

Кудінов В.А.
професор кафедри інформаційних технологій та кібербезпеки
Національної академії внутрішніх справ
к. ф.-м. н., доцент

Станом на сьогодні минуло майже 50 років від початку процесу інформатизації в системі Міністерства внутрішніх справ (далі – МВС) України. За цей час накопичений чималий досвід використання різних інформаційних та інформаційно-телекомунікаційних систем оперативно-розшукового та інформаційно-довідкового призначення. З 2005 року в системі МВС України, на